TAG CYBER

# Overview of Rogue Device Threats to the Financial Services Industry

This research note, jointed produced by TAG Cyber and Sepio, makes the case that rogue devices represent a particularly intense threat to financial service organizations. Several example threats, including to automated teller machines (ATMs) are used to show how rogue devices can be used to create negative consequences to the financial services sector, as well as other critical infrastructure sectors. The note includes detailed case studies of rogue device attack tools being used in practice.[1]

Prepared by

Dr. Edward Amoroso
Chief Executive Officer, TAG Cyber
eamoroso@tag-cyber.com

Ms. Jessica Amado
Content Specialist, Sepio
jessiea@sepio.systems

Version 1.0
October 2020

## Introduction

The notorious bank robber Willie Sutton is reported to have once claimed that he liked to target banks because "that's where the money is." The simple premise of Sutton's observation has not changed much over the years, except that traditional bank robbers have been mostly replaced by cyber criminals and electronic fraudsters. While these offensive actors are obviously guided by the lure of financial gain, the security risk to global financial services firms is exacerbated by activists who target banks to either make societal statements or to accomplish nation-state objectives against the critical infrastructure of an adversary.

Cyber security experts generally point to advanced persistent threats (APTs), distributed denial of service (DDOS), malware-based ransomware, and other familiar means of electronic breach as the primary vectors for targeting banks. This is a mostly accurate view, since so many of these types of breaches occur on a regular basis in the financial services industry. For example, in 2012, nation-state actors launched a series of DDOS attacks at commercial bank websites; in 2014, banks across the world were targeted by the Carbanak APT campaign; and in 2019, a British foreign exchange organization was hit with the Sodinokibi ransomware attack.

Somewhat less recognized by expert observers, but nevertheless still potentially devastating to the financial services industry, is the security threat introduced by so-called rogue devices. As will be explained below, the hardware or software associated with certain types of devices can be manipulated by hackers to create tampered devices that can threaten their operating environment. This security threat is generally accepted as significantly dangerous to device-rich environments such as industrial control environments such as factories. This note makes the perhaps unexpected claim that this threat is just as intense to financial services firms.

## Threats to Financial Institutions

Before getting into the details of rogue devices, it helps to highlight the security challenges in financial services. As experts know, the financial services industry is one of the most important in the world, being a primary source of economic growth and development for a country. The wide range of services offered by financial institutions means that they are an essential component to any nation, thus making this a core component of national critical infrastructure.

As such, financial institutions store a substantial amount of data on its clients, including personally identifiable information (PII), which makes financial service providers a top target for bad actors. In fact, hackers target financial service firms 300% more than businesses in other industries. It is thus not unreasonable to claim that financial services organizations are faced with billions of attempted attacks every year.

[1]*The case studies and examples used throughout this research note come from two different types of sources. First, many of the examples are easily identified in the published literature and are used to help make our case regarding rogue device risk. In addition, however, several examples stem from the practical experiences of Sepio with customers – and additional detail regarding these case references can be obtained by readers on request.*

Financial institutions are targeted for a variety of reasons. Some hacktivists believe that the industry, and those working within it, are a primary reason for many of the world's societal problems. A more common motive, however, is the financial gains that a perpetrator can benefit from when targeting this industry. Many highly skilled non-state actors are carrying out deceitful attacks for this reason.

Perhaps more concerning, however is that because of a country's heavy dependency on financial service providers, hostile states and state-sponsored actors are also conducting attacks in order to sabotage an adversary. These attacks are extremely perilous due to the advanced capabilities possessed by a state sponsor. It turns out that the use of rogue devices is becoming a more important component of these attacks.

## Rogue Device Threats – High Level Overview

Rogue devices are pieces of hardware, usually undetected by IT security teams, that have been maliciously tampered by hackers to target assets on a network of interest. Rogue devices are doctored to exploit their Ethernet or USB Human Interface Design (HID) interface to accomplish an attack objective. These devices include modified peripherals such as cameras, chargers, mice, and keyboards – and since rogue implants operate at the physical layer, it is difficult for traditional security tools to detect their presence. Such covert operation makes rogue devices dangerous for security teams protecting critical assets – as one finds obviously in banks.

Rogue devices are generally manipulated to support some malicious objective. By using the hardware attack interface, bad actors increased their chances of success since the attack can easily go undetected. Hardware implants sit on the physical layer, for example, thus going unnoticed by existing security software solutions. Spoofed peripherals will be recognized as genuine devices, while executing the attack through a USB HID interface. Spoofed MiTM network devices raise no alarms. These devices are thus threatening due to their covert characteristics. Moreover, the attacks that these devices can carry out cause serious damage to the victim.

The range of cyber security threats that can be accomplished by rogue devices is surprisingly wide, perhaps because the nature of rogue devices involves implants which can be designed to accomplish many types of attacks. Hackers can learn malicious exploit methods through the normal means including nation-state sponsored methods. These exploits are then coded into the doctored device with the goal of communicating with the external environment through the USB HID or Ethernet interface. The specific types of security threats possible using rogue devices are summarized below.

### *Rogue Device Threat: Advanced Persistent Threat (APT)*

The salient aspect of the advanced persistent threat (APT) is the lengthy duration the attack campaign remains embedded in a target system or network. APTs tend to be carried out by capable adversaries, and most experts equate the operators of such attacks with nation-state actors. The most common form of APT involves a phishing attack, followed by malware insertion, which then enables the slow traversal across the target – with the ultimate goal of exfiltrating valuable information.

In practice, APTs have also followed a somewhat different cadence – one guided by the deployment and use of rogue devices. The Carbanak attack, mentioned above, was just such a campaign – one that was in operation for two years and which resulting in over a billion dollars being stolen from banks. Carbanak worked by implanting malware into the target bank's network for the purpose of enabling automated teller machine (ATM) theft.

One Carbanak use-case involved turning ATMs into rogue devices that would dispense cash at a pre-determined time to a waiting operative. To the network security team, the ATM would appear perfectly normal, but behind the scenes, the operation of the ATM device was altered. Interestingly, security surveillance camera footage showed an individual retrieving money from a rogue ATM without ever touching the screen. This observation led to the external investigation that found the malware.

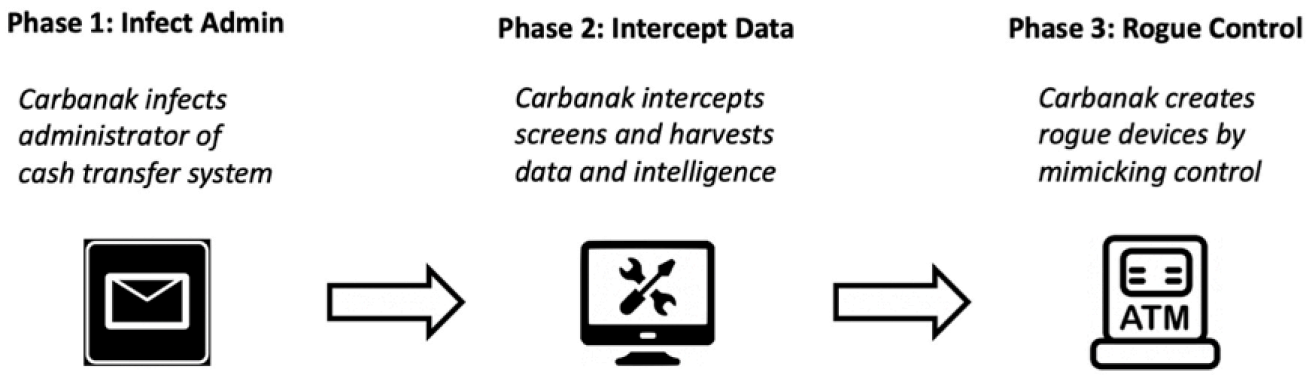


**Figure 1. Carbanak Attack Process**

### *Rogue Device Threat: Distributed Denial of Service (DDOS)*

The risk of distributed denial of service (DDOS) attack to banks is well-known. The 2012 DDOS targeting of many commercial bank websites by a nation-state sponsored actor involved traditional botnet-originated traffic. More recent incidents, such as the 2019 DDOS attack to the Hong Kong Exchanges and Clearing Limited (HKEx) followed a similar botnet-originated volumetric pattern.

More recently, however, the possibility of rogue devices initiating DDOS attacks from internal networks has emerged. Rogue Internet of Things (IoT) devices, in particular, could generate volumes internal to a financial services firm's infrastructure to clog some targeted system or network chokepoint – perhaps involving the outbound connection to the Internet. Furthermore, the use of protocols such as Bluetooth introduces risk to banking networks through campaigns that exploit flaws in pairing and other operations. The BlueBorne and Bleedingbit exploits are good examples.

### *Rogue Device Threat: Ransomware*

Virtually all financial services firms have been hit with ransomware in some form in recent years, so no effort is required to convince banks to pay attention to this risk. What might be less well understood, however, is the challenge of addressing rogue devices designed to enable ransomware attacks. These malicious use-cases are much more difficult to detect using standard cyber security tools.

An example is the use of social engineering via a poorly protected IoT device to a targeted human for the purpose of installing ransomware on a network. Since many IoT devices cannot be easily updated with patches and updates, they represent an important attack vector for organizations with valuable resources – such as banks. This is an exploit that extends to all critical infrastructure. It is reported, for example, that 70% of the Washington DC surveillance cameras were infected with ransomware in advance of the 2016 Presidential Inauguration.

***Case Study: Third-Party Hardware Risk***

The introduction of Trojan horse hardware or software to a given device – such as a motherboard on a computer – introduces interesting possibilities for an adversary. In 2018, a controversial article in Bloomberg suggested that Supermicro, an American company with deep connections to China, had inserted a listening implant onto the motherboards of the systems they sold to major hosting providers such as Amazon.

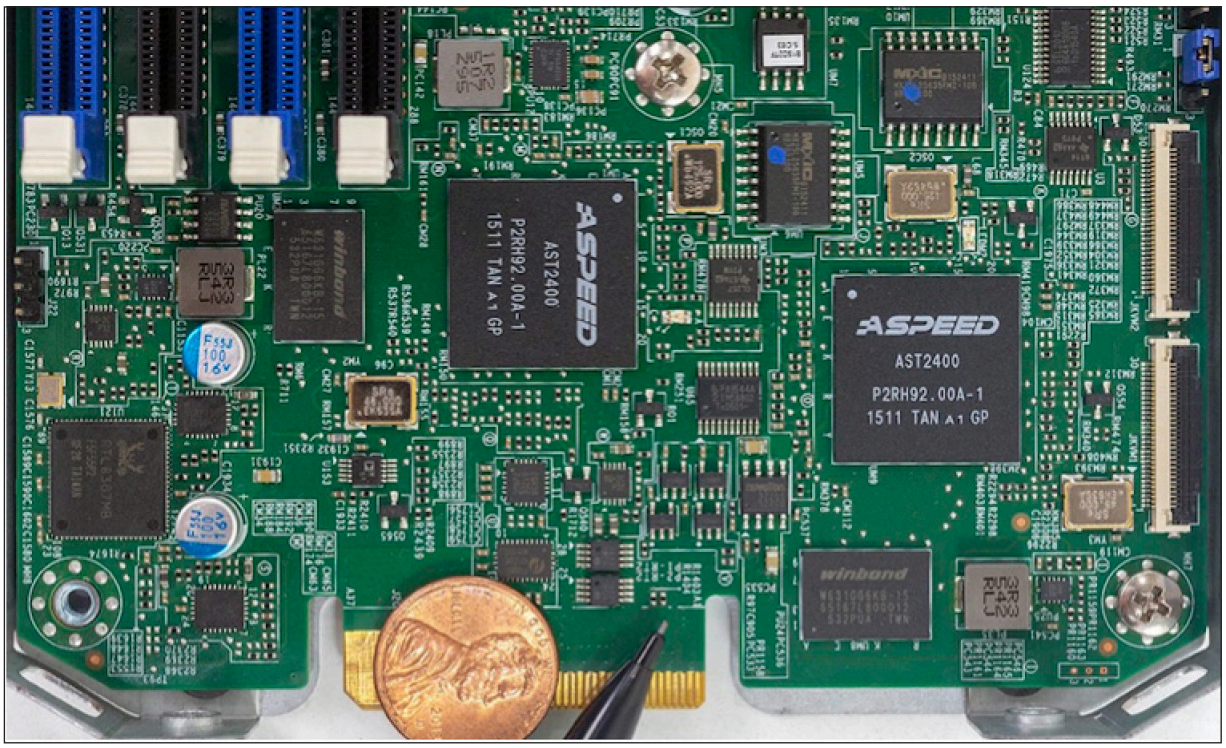


**Figure 2. Supermicro Motherboard[2]**

Subsequent investigation suggested that this attack had much greater coverage than had originally been considered. Supermicro motherboards are used across many critical infrastructure sectors, including financial services, so this attack had high potential consequence. The influence of China in the attack underscores the nation-state potential to use rogue devices to carry out attacks.

*Source: https://www.bankinfosecurity.com/where-secret-spying-chip-reported-by-bloomberg-a-11633*

# Rogue Device – Detailed Attack Case Studies

To understand in more detail how rogue device threats have actually played out in practice for financial services, it is worth digging in deeper to some case studies to highlight common themes. Studying these case studies allows security teams at financial services firms to improve their protection profile for rogue device – which will result in lower overall cyber risk. Below are some more specific, detailed descriptions of rogue devices in the context of cyber-attacks on targeted financial service and related critical infrastructure.

***BadUSB***

This HID attack gadget looks like an ordinary USB drive, except when plugged in, it emulates a USB keyboard and can be programmed to inject malware to exfiltrate data or take over the machine. There are various types of this attack tool including the USB Rubber Ducky, which has been used in several known attacks.

One attack using BadUSB occurred at the beginning of the COVID-19 pandemic. A hospitality company was given a $50 Best-Buy gift card in an envelope which also included a USB thumb drive. Once plugged in, the USB presented a list of items which could be bought with the gift card. Luckily, the company contacted security experts who identified the attack.

Unfortunately, this was not the first attack targeting hospitality. There have been previous threat actors, such as DarkHotel and RevengeHotels, which are known to be active in this industry. In one attack, a physical rogue device was used, capable of impersonating a legitimate keyboard which goes “below the radar” of existing EPS/EDR solutions. Diving deeper into the physical layer is the best means for providing protection against this type of attack.

In one investigation by a cybersecurity firm, BadUSB device was discovered functioning as a keyboard and performing keystrokes to launch commands to download and install malware. To install the malware, the device triggered keystrokes to launch a PowerShell command, which then downloaded a more cumbersome PowerShell script, ultimately leading to the malware being installed.

To the human eye, the USB device looked normal. The BadUSB device used an Arduino microcontroller ATMEGA32U4 had been programmed to act as a USB keyboard, thereby allowing it to be trusted. However, the purpose of this device is to surreptitiously type malicious commands, in this case causing the installation of malware.

It is almost impossible to detect this type of attack, as these devices are recognized as genuine HIDs by existing security software solutions. Therefore, anti-virus scans will not present any indication that a malicious attack is underway. Anti-virus software might be able to detect the malware injected by the BadUSB, provided that it is a known variant, however this is not a sufficient solution.

In one investigation into BadUSB attacks, it was found that 5 of 16 anti-virus tools detected the injected malware. Furthermore, the tools which were able to detect the malware were unable to detect the presence of the malicious hardware device. The alternative is to employ advanced forensic methods such as physically taking apart and reverse engineering the device, yet this is impractical as there are thousands of devices being used by organizations.

Ideally, an organization will want to employ a security software solution that detects these hardware attacks; something which vendors such as Sepio Systems have developed successfully. These attacks have occurred in the United States, United Kingdom, Germany, Russia, Israel and many more countries. The extent to which BadUSB malware can spread throughout the victim's network increases the peril of the attack, with one investigation demonstrating that an average of 325 new bots became infected per day with malware from one campaign.

***USB RubberDucky***

Another attack tool, called USB RubberDucky, also looks just like an ordinary and innocent USB drive, but plugging it into a computer can install backdoors, exfiltrate documents, or capture credentials – all by injecting keystrokes at superhuman speeds. Since 2010, when keystroke injection was invented, the USB RubberDucky became the must-have penetrated testing tool.

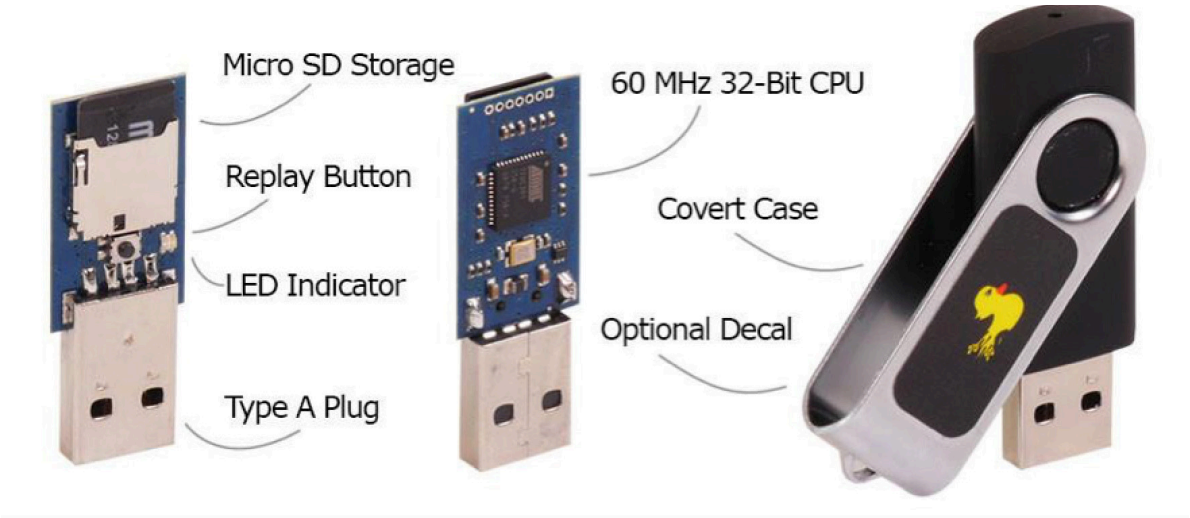


**Figure 3. Schematic of USB RubberDucky Device[3]**

One incident involving USB RubberDucky occurred in 2019 when a Chinese woman named Yujing Zhang entered the Mar-a-Lago resort claiming that she had entered to use the swimming pool (even though she had no bathing suit). She also claimed that she was there to attend a United Nations Chinese American Association event, yet it was later found out that such event did not exist. Suspicion led to her arrest, and it was discovered that Zhang had been carrying two Chinese passports, a laptop, four phones, and a USB RubberDucky drive. Following this discovery, Secret Service agents tested the device and found that was infected with malware.

RubberDucky specifically uses keyboard emulation to execute a covert channel communication stack. By creating an out of-band connection using the device's wireless interface, an air gap can be bypassed. Spoofed Peripherals require minimal current consumption which can be supplied by the host PC, allowing perpetrators to perform network packet sniffing and to exfiltrate information out-of-band remotely due to the integrated Wi-Fi functionality.

[3]*Source: https://shop.hak5.org/products/usb-rubber-ducky-deluxe*

In this case involving Zhang, the information that could have been obtained could have been extremely sensitive since the resort belongs to the US President. Humans pose a huge risk to security and, in this case, social engineering techniques were evidently used for Yujing Zhang to gain access to the resort. Zhang took advantage of her language barrier and was granted access by the staff, which allowed the malicious device inside the premises.

Studies show that 53% of malware attacks in organizations are a result of careless or uniformed staff. It was evident that the staff in this case was unaware of the risks that can come with allowing unauthorized individuals inside. Once inside, Zhang could have easily used the device herself on one of the computers, or merely left it on the premises with the hopes that it would be picked up by an unsuspecting employee on the resort's computer themselves.

***USBCulprit***

Another rogue device tool recently revealed is called USBCulprit, which has been used by cybercrime organizations such as the Chinese threat actor known as Cycldek, first identified in September 2013. In previous campaigns, this group has targeted entities in Southeast Asia using diverse malware variants such as PlugX and HttpTunnel. Data published by Kaspersky Labs indicates that this tool has been found to rely on USB media to exfiltrate victim data, which may suggest that Cycldek is attempting to reach air gapped networks in victim environments or that they are relying on physical presence for the same motive.

Once USBCulprit is loaded to memory and executed, it operates in three phases. First, the environment is prepared for the malware to be disseminated. Second, the malware seeks to intercept the connection of new media and verify that it corresponds to a removable drive. Third, the malware begins lateral movement throughout the network. The USBCulprit is able to scan multiple paths, collect documents with specific extensions (*.pdf, *.doc, *.wps, *docx, *ppt, *.xls, *.xlsx, *.pptx, and *.rtf) and export them to a connected removable drive.

The malware was designed to duplicate itself to certain removable drives in the presence of a certain file, which proposes that it can be spread laterally to other systems by simply inserting the infected USB drive. Kaspersky's telemetry revealed that this USBCulprit tool was first found in 2014, although the latest samples were only detected in 2019.

***USBNinja Cable***

The USBNinja was created by the RFID Research group in 2018. It looks and functions just like a regular USB cable, except that it can deliver choices of attack payload to the host machine. The USBNinja can be viewed as the next step in the evolution of BadUSB, embedding the attack in the USB cable itself. It can emulate keyboard and mouse actions. Additionally, payloads can be customized and can be highly targeted.

USBNinja Cable is undetectable by firewalls, AV software, or visual inspection. It is an ideal tool for penetration testers, police, and the government. However, importantly, this tool is highly appealing for bad actors seeking to cause substantial damage. Moreover, the device is available for only about $180USD, which includes the complete kit of the USB cable, magnetic ring, and BTLE control. This relatively low price, and easy access to acquiring the device, makes it a highlight attractive tool for attackers.

***Raspberry Pi***

A Raspberry Pi is a pocket-sized computer that connects to the Internet and can be bought for as little as $25USD. This device was originally developed with the intention of providing a low-cost computer and free software to students. However, it is now also being used with malicious intent as hackers utilize this device, not only because of its convenient tiny size, but also for the range of hacking tools that it provides, notably being able to capture data on target networks.

The Raspberry Pi supports a variety of payloads and scripts, and once mounted, it can perform network packet sniffing, perhaps for reconnaissance. Some more advanced payloads include an 802.1x bypassing module, which helps the attacker overcome various MAC authentication procedures used by some NAC vendors. Exfiltration of the data from the Raspberry Pi can easily be done by connecting a mass storage device to it, using its on-board Wi-Fi capabilities or, for more covert operations, a dedicated USB-Wireless Dongle (non-Wi-Fi), making its detection more difficult.

This small device has been used to carry out many rogue device cyberattacks, including the attack on NASA in April of 2018. The hackers went unnoticed for almost a year, and it was only announced in 2019 that NASA had been breached. Even after this late discovery, the damage was done, and it was too late. The hackers stole about 500 megabytes of data from 23 files, two of which contained information related to a Mars mission.

According to a June report by the Office of the Inspector General about cybersecurity at NASA's Jet Propulsion Laboratory, the Raspberry Pi computer that had been used was not authorized, but even so, it was connected to the lab's network. It was also found in the report that the agency had reduced visibility into devices connected to its network, which hindered the ability to comprehensively secure those networks. By targeting this Raspberry Pi, the hackers were able to gain access to the network, which showed a major weakness. It can cause crucial damage if unauthorized devices such as these can be added to the network without even being identified. When news broke of this attack, several connected agencies disengaged from the network to prevent further damage.

An additional case in which the Raspberry Pi has been used involved researchers finding classified operational documents belonging to a large US-based natural gas utility-operator. This was part of academic security research that included the scanning of repositories of files. When approached by the researchers, the utility's security team was surprised to discover that the documents were authentic and there was no internal evidence that had been removed. The network containing the stolen documents was air-gapped, so there was no possibility that they were leaked through the Internet. The use of all removable media was also strictly blocked so the option that someone saved a copy of the document and taken it out was ruled out.

The investigation concluded, however, that the internal critical network was no longer air-gapped and that it had been breached. The network was therefore not only vulnerable to exfiltration, but also to injection and sabotage. When plugged in, the infected device was detected by the host PC as a combination of a fully functional mouse and HID keyboard- USB Class 3, Subclass 1, Protocol 1. Using keyboard emulation, the HID interface typed a PowerShell script which built and executed a covert channel communication stack. By creating an out-of-band connection using the infected mouse's wireless interface, the air gap was bypassed.

Despite keyboards being viewed primarily as input devices, one should be aware that the bidirectional communication channel for controlling keyboard functionality can also be used to exfiltrate data from an enterprise. In this attack, the Raspberry Pi Zero W can be used to ensure not only a minimal consumption that can be easily supplied by the host PC (being the target of the attack), but also allows perpetrators to perform network packet sniffing and exfiltrate information out-of-band remotely due to its integrated Wi-Fi functionality.

The Sepio team has discovered devices that are not based on Wi-Fi communications, but instead using LoRanWAN (wide area low power wireless network) modules for remotely communicating with Rogue Peripheral Devices. When connected, the mouse is detected as a legal and safe USB hub, to which both the mouse and Raspberry Pi Zero W are connected. A wide collection of penetration testing images and utilities are available for Raspberry Pi, ranging from keyboard emulators (rspiducky), through traffic hijackers (PoisonTap), and backdoor full remote access implementations. Keyboards can also be utilized in the same way to carry out attacks for infection purposes or to exfiltrate sensitive information. Again, these will be recognized as genuine HIDs.

***Proxicast PocketPort 2***

The PocketPort 2 is the world's smallest 3G/4G/LTE USB Cellular Modem to Ethernet Bridge which can function as a 3G/4G modem or mini 3G/4G router. This device instantly connects virtually any cellular 3G/4G (LTE, HSPA+) USB modem to any Ethernet device by plugging both devices into the PocketPort 2. Additionally, it is easily portable, simple, and low-cost as opposed to large, complex, and expensive cellular Ethernet modems. The PocketPort 2 mobile router from Proxicast was used in several attacks, one of the most substantial attacks being on a Tier 1 bank.

In this case, the Tier 1 bank audit revealed irregularities, and it became evident that an external party had continuous access to the internal and secured parts of the network. After investigating the computing assets of the bank, such as the servers, the desktop workstations and management's laptop for malware with remote access capabilities, nothing was discovered. Subsequently, investigations focused on deep monitoring of the ingoing and outgoing communications from the network hoping there would be an indication as to what was occurring. Again, no evidence was found for the full remote access.

The Cyber Investigations Practice of a leading global consulting firm was then approached for assistance. Their team found that an authentic laptop belonging to the bank was cloned and connected to the network infrastructure via an out-of-band channel in parallel to the existing and legitimate laptop. The network access profile and envelope, in addition to the certificate, were authentic and valid, meaning that none of the existing security and monitoring tools recognized it as a Rogue Device. The attackers were using a "ghost" malicious device that was acting in the shadow of the legitimate one.

Upon further investigation, a small, unidentified rogue hardware device was found to be installed in one of the distribution cabinets and was providing the perpetrator with remote access capabilities, with the existing security measures completely oblivious. No one knew what this device was, what it was doing, who brought it in, and when. The attackers used a legitimate off-the-shelf network router sold by a third party.

Besides its other modus operandi, the device supports a virtual cable mode whereby two devices can be paired, and each installed at different locations while operating as if they are interconnected using a standard passive LAN cable. The two devices are able to reroute and tunnel the communication via a simple switchboard application, allowing traffic to be intercepted and data packets to be injected and streamed back into the network, in addition to being able to carry out more complex man in the middle (MiTM) attacks. These devices do not have an IP or MAC address, meaning that Intrusion Detection Systems (IDS), Network Access Control (NAC) and Network Monitoring tools are unable to detect them.

The entire manipulation is conducted on the Physical Layer (Layer 1) and the Data-Link Layer (Layer 2), so all higher-level communications are considered authentic and safe. In this specific incident, the tool used was the PocketPort2 mobile router from Proxicast. The device pair was configured to run in virtual cable mode and to use a private switchboard server to ensure that there would be no traces back to the origin of the attacker.

Sepio, in particular, has also been able to detect and mitigate similar types of attacks that were conducted using different tools that acted in a similar manner. Examples of such devices are mAP lite and AR150, both purchased legally from reputable vendors. Theoretically, any hardware platform with an operating system and set of drivers that support promiscuous mode and the ability to directly transmit data packets (raw sockets) can be adapted to act as a rogue device. Stolen data can be leaked through local storage or an out-of-band communication channel (preferably wireless) without being detected by current network security tools, such as IDS and NAC.

***ATM Attacks***

Cyberattacks on ATMs come in various forms. First and foremost, there is the ATM-specific malware attack, exemplified by CutletMaker, Ploutus D, and ATM Proxy, which bypass cash dispenser logic and are triggered by a connected keyboard or cellphone. The other two forms are attacks with specific hardware. The first is called a Blackbox attack, which is becoming more and more common. There have been recent reports of this type of attack on banks across Europe. In this attack, the ATM PC is replaced for direct communications with the cash dispenser and is triggered by a smartphone (nearby Bluetooth). The other form of specific hardware attack is by using Network Implants, which creates a fake processing server and provides cross network infection.

As attackers are finding out that physical access to the internals of the ATM is becoming more difficult to achieve, a new method of attack has been introduced; external implants, which are becoming more popular and common. In most cases, they are off-the-shelf-devices, mainly cellular routers, modified in such a way that they operate in “transparent/bridge” mode without having any L2 (MAC) presence. As such, they cannot be picked up by NAC/IDS solutions.

## Consequences of Rogue Device Threat

The threat implications of rogue devices on financial services firms can be considerable, especially when the attack is carried out by capable adversaries such as nation-state actors. While soft consequences such as reputation must always be expected after an attack of this type, the more tangible implications of rogue device security attacks on the financial services industry are as follows:

- Direct Financial Loss – When rogue device attacks target ATMs and other systems that can dispense cash immediately, the financial losses are direct and immediate. It is not difficult to imagine this being done at scale and in a manner that creates a large aggregate loss.
- Indirect Financial Loss – When rogue devices are discovered and reported within a bank or other financial institution, it can have a negative impact on present and future consumer and commercial business. Just a tiny percentage hit can result in a considerable loss.
- Response Costs – Preventing rogue devices is easier and cheaper than finding and addressing their consequence after an attack. The incident management costs of rogue device attacks can thus lead to considerable operating expenses to respond, report, and remediate.
- Compliance Costs – Since financial service firms are regulated, the compliance costs to report, fix, and provide evidence to external entities will be considerable for rogue device attacks. Again, the compliance costs will be lower to detect than to respond.

## Action Plan

Any financial service organization that has not previously addressed the potential for rogue device attack to their systems and infrastructure is advised to do so immediately. The manner in which this can and should be done will vary from one organization to another, but some general action plan elements can be identified. Below we list a few actions that should be part of any process to address rogue device risk in financial services:

***Commercial Technology Review*** – The team managing the commercial cyber security portfolio should immediately identify a list of vendors who provide detection and prevention of rogue device risk. TAG Cyber analysts provide this type of portfolio services and are willing to help.

***Threat Modeling*** – The security team should weave rogue device risk into their normal threat modeling process to accurately identify the local consequences of an attack. This should include both soft and tangible consequences in the analysis.

***Implementation Plan*** – A plan to test rogue device detection and risk management into the applicable services and infrastructure should be created. This is likely to include a proof-of-concept project that can help determine effectiveness. TAG Cyber can help here as well.